8 Phishing Lures Preying on Pandemic Panic

darkreading.com/attacks-breaches/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495

Attacks/Breaches

Phishing campaigns and scams are skyrocketing to take advantage of people concerned about COVID-19 impacts. Here are some key examples in action.

Image Source: Adobe (helfei)

There's no rest for the weary, especially not for cyber defenders protecting their colleagues, friends, and families from threats amid the COVID-19 crisis. Cybercriminals continue to put the screws to victims, adding onto their typically busy slate of attacks a host of new coronavirus-driven attacks. As with any global event or crisis, the bad guys are jumping on the opportunity to take advantage of fear, distraction, and interest in COVID-19 to craft particularly compelling scams. In particular, they've tailored their phishing lures to prey upon pandemic panic. Here are some examples that researchers have dug up over the past several months as the situation persists.

Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading.

8 Phishing Lures Preying on Pandemic Panic

DR darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495

Attacks/Breaches

Phishing campaigns and scams are skyrocketing to take advantage of people concerned about COVID-19 impacts. Here are some key examples in action.

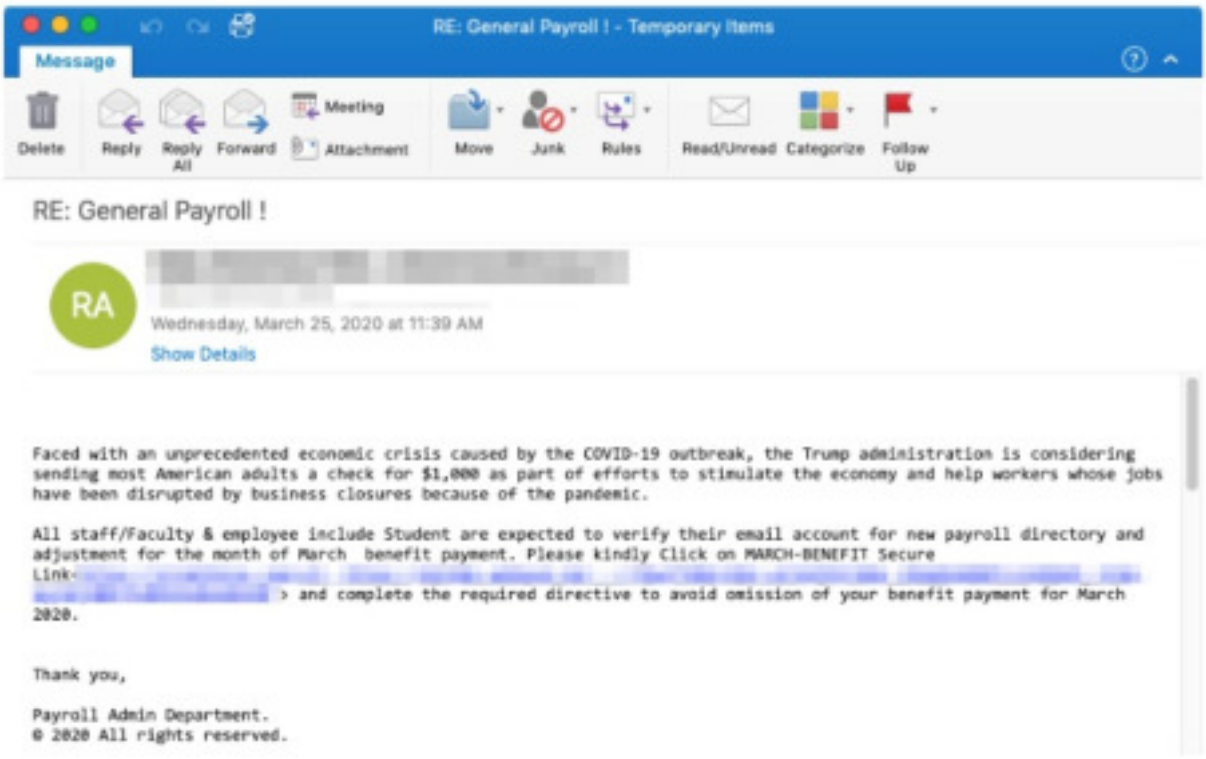


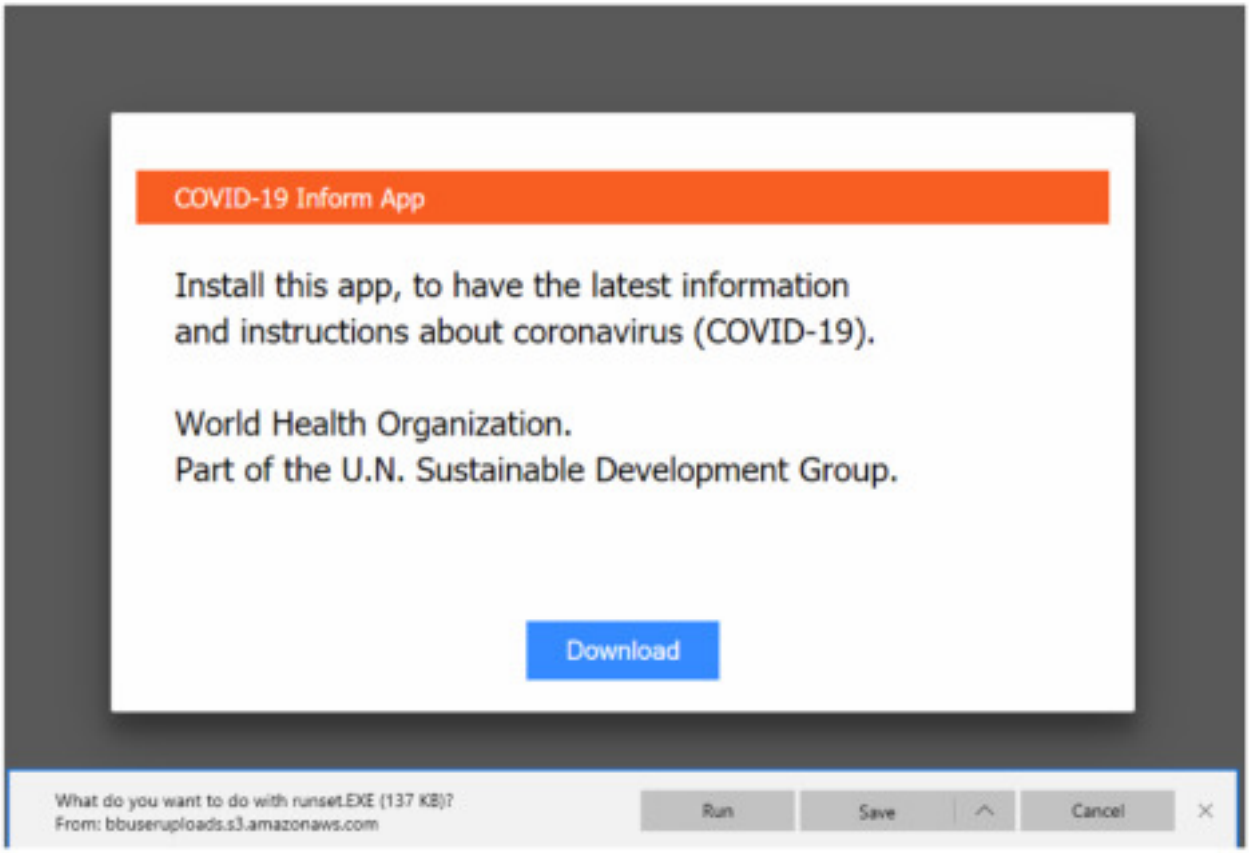
Figure 1 US Payroll COVID-19 Relief Lure

Government Relief Fund Scams

As government representatives have started to enact legislation to provide relief funds for those left unemployed or otherwise financially impacted by COVID-19, criminals have ramped up phishing ploys that look like government correspondence about those funds to trick people into giving up their credentials. According to research released by Proofpoint on April 1, these kinds of scams are targeting citizens in the US, UK, and Australia, among others.

8 Phishing Lures Preying on Pandemic Panic

DR darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495



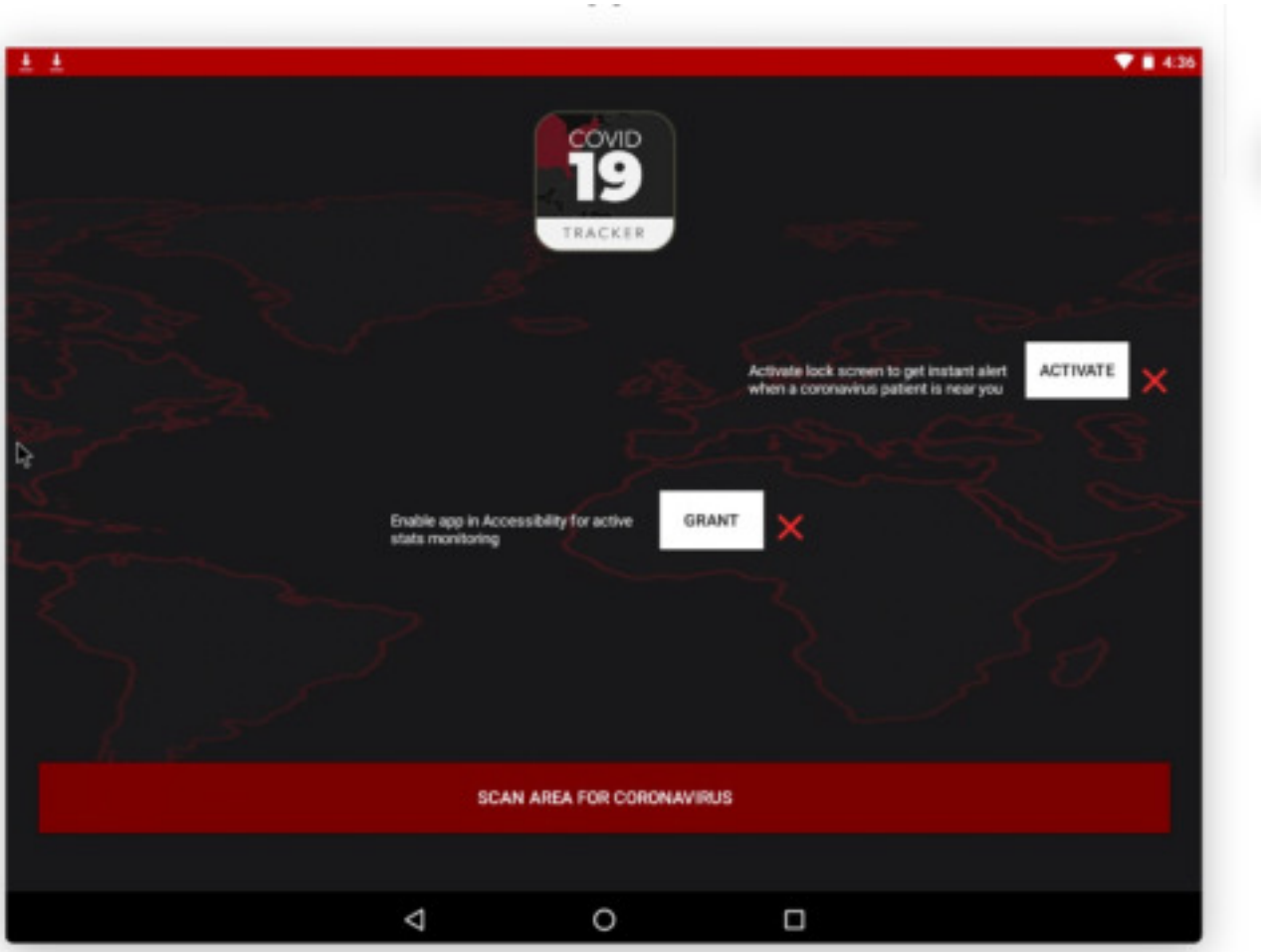
DNS Hijacking Nudging to Phishing Sites

Toward the end of March, researchers at Bitdefender said they discovered targeted DNS hijacking attacks against the kinds of home routers that legions of new work-from-home employees depend on for connectivity. The attacks redirect users to coronavirus-themed Web pages that are armed with malicious infostealer payloads disguised as COVID-19 informational apps.

(Image Source: Bitdefender)

8 Phishing Lures Preying on Pandemic Panic

DR darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495



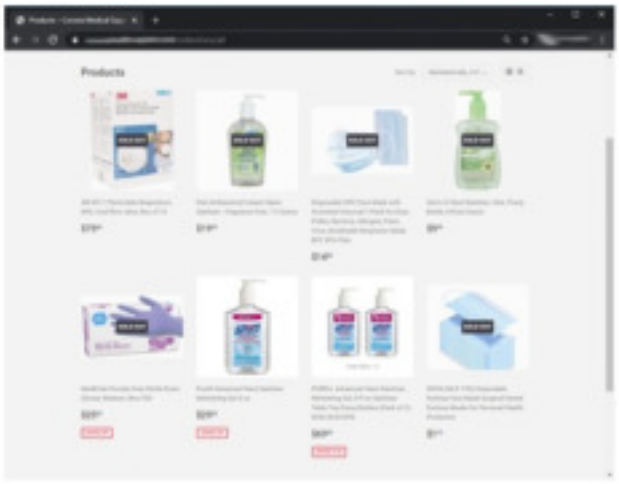
Coronavirus Tracking App Ransomware

In mid-March researchers with DomainTools found that attackers are creating bogus COVID-19 tracking apps booby-trapped with ransomware. Dubbed CovidLock, the example they found worked by using a screen-lock attack against Android phones that forces a change in the password governing the device's screen-lock capabilities.

(Image Source: DomainTools)

8 Phishing Lures Preying on Pandemic Panic

darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495



Face Masks and Medical Supplies

Similar to testing kits, face masks and other hard-to-find medical supplies are being used as a favorite carrot for phishing attempts and good-old-fashioned fraud. In early March, Bitdefender researchers ran through a range of new sites that were cropping up with promises of deep discounts on masks and other supplies. Many of them also promise limited-time offers and ask for Bitcoin payment to set the hook nice and firmly with desperate victims.

(Image Source: Bitdefender)

8 Phishing Lures Preying on Pandemic Panic

darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495

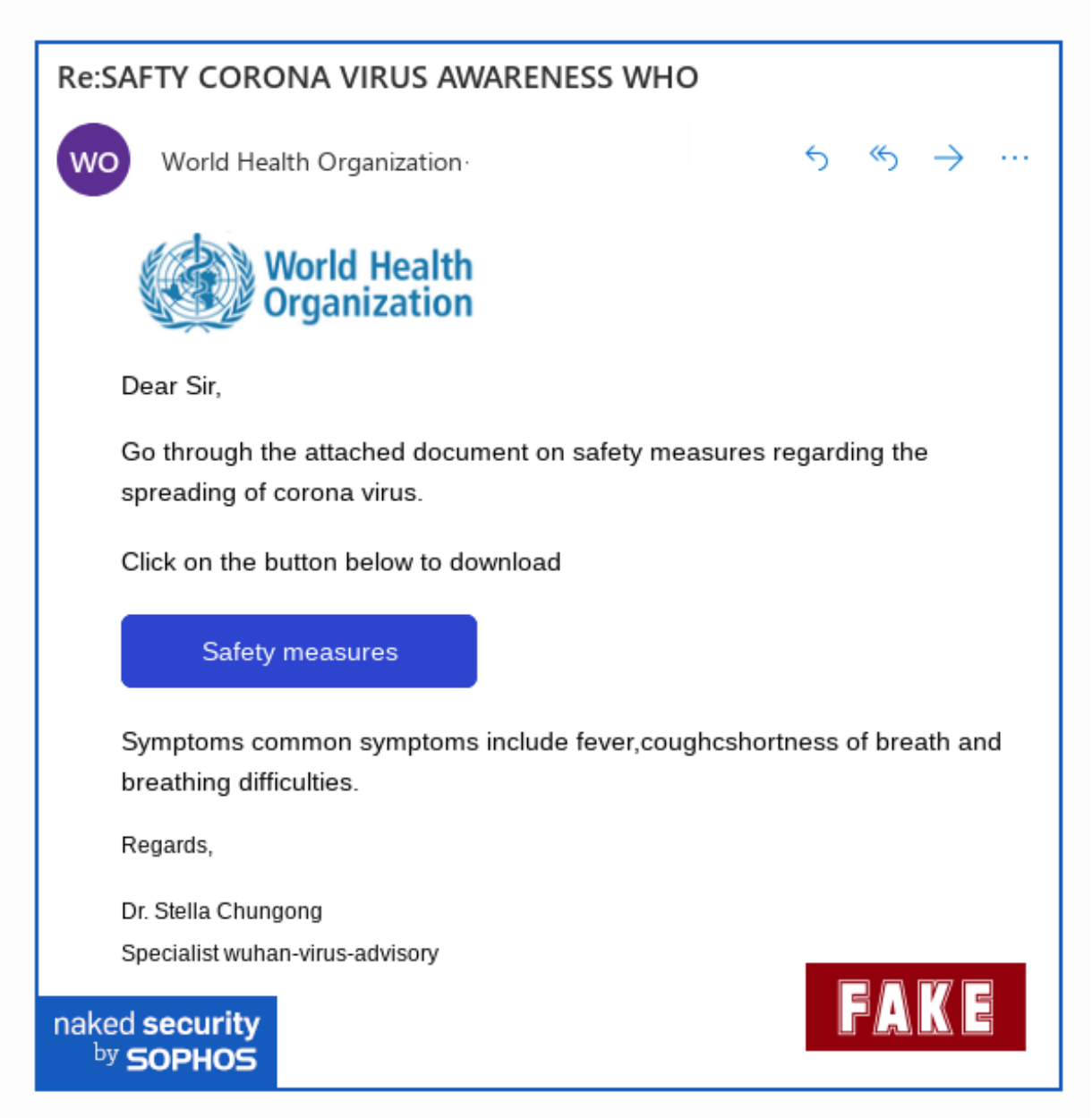
COVID-19 Testing Kit Scams

The bad guys are taking advantage of keen interest in COVID-19 testing to run a variety of scams around the availability of testing kits. These are spanning across not just email but also robocalls, according to the Federal Communications Commission (FCC), and text message smishing attempts, according to the Better Business Bureau (BBB). According to the FCC, it has run across a range of other robocall scam lures tied to the coronavirus, including work-from-home opportunities, student repayment plans, and debt consolidation -- some of which aren't just targeted toward consumers but also small businesses.

(Image Source: Adobe (Parilov))

8 Phishing Lures Preying on Pandemic Panic

darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495



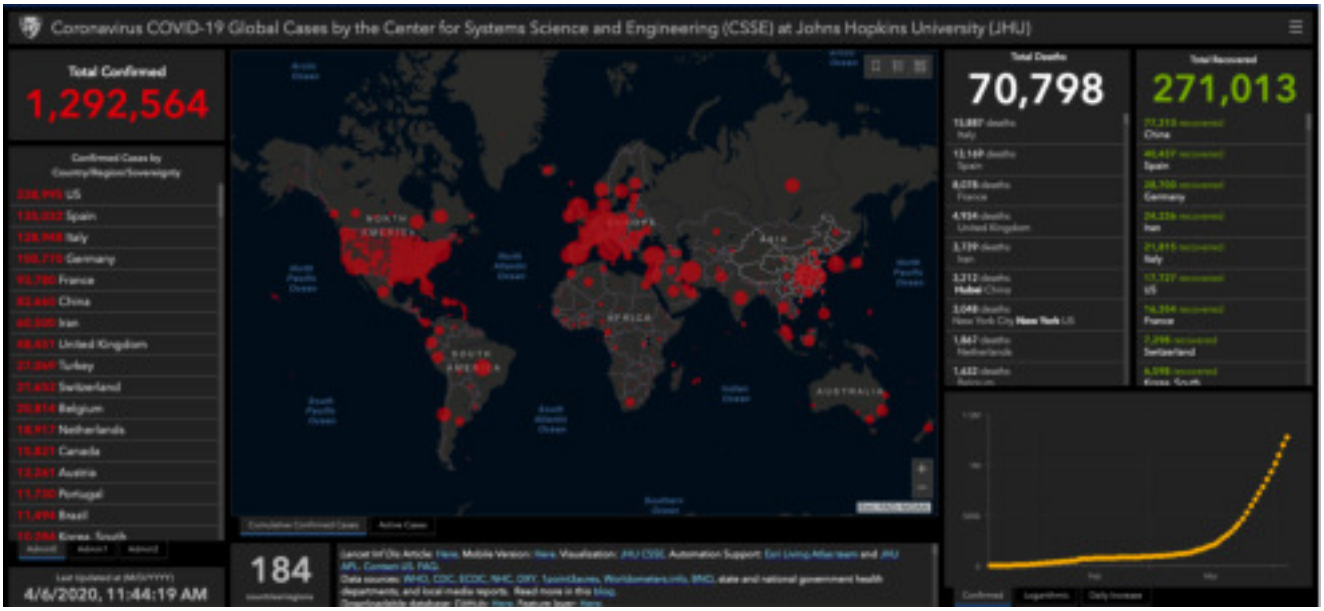
Impersonation of Official Health Organizations

Savvy criminals have been particularly focusing on piggybacking off of the legitimacy of official organizations, such as the Centers for Disease Control (CDC) and the World Health Organization (WHO), to design a range of different phishing lures. As early as February, Sophos researchers were reporting on fake advisory emails that were using the urgency of the situation to trick users into divulging credential information.

(Image Source: Sophos)

8 Phishing Lures Preying on Pandemic Panic

darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495



Malicious Infection Maps

Attackers are taking advantage of public interest in to-the-minute infection maps from the likes of Johns Hopkins to create compelling lures for malicious campaigns. Like the watering hole campaigns, these don't have to rely on email campaigns, MalwareBytes researchers say. Instead, the bad guys are standing up malicious websites using AzorUlt infostealer malware that is hidden behind a legitimate-looking infection map. According to KrebsOnSecurity, many bad guys are ramping up with the use of a Java-based malware kit, sold for $700, that uses the Johns Hopkins map as its lure.

(Image Source: Coronavirus.jhu.edu)

8 Phishing Lures Preying on Pandemic Panic

DR darkreading.com/8-phishing-lures-preying-on-pandemic-panic/d/d-id/1337495

H奶[redacted]辣曬性感寫真 雙腿夾緊鴻「神秘黑三角」	[redacted]	2/3/2020 9:01	9
最美空姐[redacted]操翰慢 錯過千年一遇美女		27/2/2020 11:56	2
最美空姐[redacted]操翰慢 錯過千年一遇美女		27/2/2020 9:47	0
H奶[redacted]辣曬性感寫真 雙腿夾緊鴻「神秘黑三角」		27/2/2020 9:42	0
35E香港女星滯留韓國被催快回家		26/2/2020 15:44	1
35E香港女星滯留韓國被催快回家		26/2/2020 15:17	0
鋼琴女神辣穿比基尼洗超跑[redacted]車模美胸見客		26/2/2020 9:09	1
[redacted]巨乳羞頂「[redacted]」網友對[redacted]的憎恨指數爆增		25/2/2020 9:41	0
[redacted]巨乳羞頂「[redacted]」網友對[redacted]的憎恨指數爆增		25/2/2020 9:40	0
網友爆料95後女星[redacted]潛[redacted]、[redacted]玩入院		24/2/2020 15:49	2
[redacted]遊樂園兩腿大開！一彎腰...超兇奶彈震撼滑出		21/2/2020 19:55	5
超辣！[redacted]無碼泡澡照曝光 S型「窈窕曲線」宅宅噴鼻血惹～		21/2/2020 9:21	0
AV女優霸主是誰？ 老司機推薦名單曝光		20/2/2020 17:24	0
AV女優霸主是誰？ 老司機推薦名單曝光		20/2/2020 17:22	0
最美空姐穿上制服「重回老本行」網回憶湧現：漂亮		20/2/2020 15:49	0
【武漢肺炎】封城致供應鏈斷裂 港商：香港或陷物資短缺		20/2/2020 15:45	1
香港女模陪男友被困武漢 遭同鄉嗆「死了不值得可惜」		19/2/2020 20:12	2
香港女模陪男友被困武漢 遭同鄉嗆「死了不值得可惜」		19/2/2020 19:52	1
香港女模陪男友被困武漢 遭同鄉嗆「死了不值得可惜」		19/2/2020 19:52	0
香港女模陪男友被困武漢 遭同鄉嗆「死了不值得可惜」		19/2/2020 19:47	0

Figure 2. List of news topics posted by the campaign

Figure 3. Forum post with the link to malicious site

Forum-Posted Watering Holes

In March, researchers with Trend Micro discovered a watering hole attack that targeted iOS users in Hong Kong using poisoned local news links to execute malicious mobile malware. The links were legitimate news sources that were seeded on numerous online forums through legitimate-looking posts about local developments, but the links themselves

contained hidden iframes to load and execute malicious code targeting vulnerabilities in certain iOS versions. The attack leads to a malware variant called LightSpy being loaded on victims' devices.

(Image Source: Trend Micro)